REMARKS

The Office Action mailed May 31, 2005 has been received and reviewed. Claims 1-59 are in the case. Claims 1-25 and 36-59 stand rejected under 35 U.S.C. 101 as non-statutory subject matter. Claims 1-37 and 42-59 stand rejected under 35 U.S.C. 103(a) as unpatentable over Vanstone (Vanstone et al., US Patent 6,141,420) in view of Koyama (Koyama et al., Elliptic Curve Cryptosystems and Their Applications, reference U). Claims 38-41 stand rejected under 35 U.S.C. 103(a) as unpatentable over Vanstone in view of Koyama and further in view of Elkies (Explicit Modular Towers, reference V).

By this paper, Applicant has amended claims 1, 29, and 59 to more particularly point out and distinctly claim the novel and nonobvious subject matter of the invention. For the reasons set forth below, Claims 1-59 are believed to be in condition for immediate allowance. Favorable reconsideration of the application in view of the following remarks, is therefore respectfully requested.

REJECTION OF CLAIMS 1-25 and 36-59 UNDER 35 U.S.C. 101 FOR NON-STATUTORY SUBJECT MATTER

Claims 1-25 and 36-59 stand rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Independent Claims 1 and 59 have been amended to more clearly claim the subject matter of the invention.

The Office Action asserts that "Claims 1 and 59 are directed to manipulating points on an elliptic curve". Although this manipulation is part of Claims 1 and 59, there are additional elements present in each Claim:

Claim 1 includes "generating a signal having a distinct characteristic using the selected elliptic curve method; providing substantive content; and manipulating the substantive content using the distinct characteristic." This manipulation of substantive content is a useful process, and the other elements of the Claim make it a new and useful improvement of a useful process. Even though the invention uses some complex mathematics, it achieves a useful result. This makes it more than an abstract idea. Claim 59 includes some of the same elements, and finishes with "manipulating the substantive content using the

distinct characteristic". Thus Claim 59 is also directed to achieving a useful, non-abstract, result.

Applicant submits that the amended Claims 1 and 59 describe useful processes, and respectfully requests withdrawal of this ground for rejection. Claims 2-25 and 36-58 depend on Claim 1, and were rejected under the same rationale. Applicant respectfully requests withdrawal of this ground for rejection for Claims 2-25 and 36-58.

REJECTION OF CLAIMS 29-35 UNDER 35 U.S.C. 101 FOR NON-STATUTORY SUBJECT MATTER

Claims 29-35 stand rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Independent Claim 29 has been amended to more clearly claim the subject matter of the invention.

Claim 29 is directed to a computer-readable memory storing operational and executable data. The Office Action asserts "the collection of information does not fall within the classes listed in 35 USC 101".

However, Claim 29 as amended describes a useful machine within the meaning of 35 U.S.C. 101. For example, this

machine can cause the encryption of information, a useful result.

Applicant submits that the amended Claim 29 describes a new and useful machine, and respectfully requests withdrawal of this ground for rejection of Claim 29. Claims 30-35 depend directly or indirectly on Claim 29, and were rejected under the same rationale. Applicant respectfully requests withdrawal of this ground for rejection for Claims 30-35.

REJECTION OF CLAIMS 1-37 and 42-59 UNDER 35 U.S.C. 103(A), OVER VANSTONE IN VIEW OF KOYAMA

Claims 1-37 and 42-59 stand rejected under 35 U.S.C. 103(a) as unpatentable over Vanstone (Vanstone et al., US Patent 6,141,420) in view of Koyama (Koyama et al., Elliptic Curve Cryptosystems and Their Applications, reference U).

The Office Action rejects Claim 1 as an obvious combination of Vanstone with the teachings of Koyama.

But Vanstone and Koyama cannot be combined. Both references discuss elliptic curve cryptosystems, but the details make the two systems incompatible.

Vanstone uses elliptic curves over the finite field GF[2^m], and uses the elliptic curve equations

$$Y^2 + XY = X^3 + AX^2 + B$$

and $$Y^2 + AY = X^3 + BX + C.$$

(Cover page of the Vanstone patent, first sentence of the Abstract, and column 2, line 29 of the patent text, and column 4, line 1; also see subsection (a) of Claim 1.)

Koyama uses elliptic curves over the finite fields (modulo P) and (modulo Q), with P and Q large primes so that P*Q is infeasible to factor, and also curves over the ring (modulo P*Q). Koyama uses the elliptic curve equation

$$Y^2 = X^3 + AX + B.$$

(equation 1, page 50, section 2 of Koyama).

Koyama explicitly excludes P=2 (first sentence of section 2, page 50), while Vanstone uses exclusively P=2. This alone makes the two systems incompatible, but there are further problems.

It is an important element of Koyama's methods that the orders of the elliptic curves are generally independent of some of the coefficients in the curve equations. (page 51,

section 3, Note c, last sentence.) This is completely different from the Vanstone system, where the curve order depends critically on the exact coefficients A and B in the curve equation.

Koyama's halving algorithm only works for the particular primes described in his Case 1 and Case 2 (section 2, page 51, middle of left column, and section 4.2, page 53, Theorem 5) and doesn't apply to prime power finite fields such as Vanstone's GF[2^m].

Even if this obstacle were overcome, Koyama's halving algorithm is very slow compared to the methods in Vanstone: Although Koyama's halving algorithm is polynomial time, it requires scores of point doubling and addition operations to compute the point multiples required in steps 3 and 4 of the algorithm (page 53). It would make no sense to combine such a slow method with the much faster operations used in Vanstone.

These two systems cannot logically be combined, and selected elements from Koyama cannot be imported into Vanstone because they won't work. Since neither reference suggests the combination of these two systems, and in fact the two systems can't be combined, the combination cannot be regarded as obvious.

Applicant submits that Claim 1 is not anticipated by the

illogical combination of Vanstone with Koyama, and requests withdrawal of this ground for rejection.

The Office Action also rejects Claims 26 and 29 on the same basis as Claim 1, by combining Vanstone and Koyama. As explained above, the combination of these two systems is illogical, and cannot be considered obvious.

Applicant submits that Claims 26 and 29 are not anticipated by the illogical combination of Vanstone with Koyama, and requests withdrawal of this ground for rejection.

The Office Action rejects Claim 59 as an obvious combination of Vanstone with Koyama, asserting that Koyama teaches one or more ambiguous point triplication steps, and testing whether a point is twice halvable to resolve an ambiguity.

But Koyama makes no mention of triplication, nor of testing whether a point is twice halvable, nor of resolving an ambiguity. Page 52, section 4.1, right column, Note (b) mentions an ambiguity, but no method of resolving it. The elements needed from Koyama to defeat Claim 59 are missing, even apart from the incompatibility of Vanstone with Koyama.

Applicant submits that Claim 59 is distinguished over the combination of cited arts, and requests withdrawal of this ground for rejection.

Claims 2-25, 36-37, and 42-58 depend directly or indirectly on Claim 1. Claims 27 and 28 depend on Claim 26. Claims 30-35 depend directly or indirectly on Claim 29. Applicant requests withdrawal of rejections of the dependent Claims 2-25, 27-28, 30-37, and 42-58.

REJECTION OF CLAIMS 38-41 UNDER 35 U.S.C. 103(A), OVER VANSTONE IN VIEW OF KOYAMA AND IN VIEW OF ELKIES

Claims 38-41 stand rejected under 35 U.S.C. 103(a) as unpatentable over Vanstone (Vanstone et al., US Patent 6,141,420) in view of Koyama (Koyama et al., Elliptic Curve Cryptosystems and Their Applications, reference U) and further in view of Elkies (Explicit Modular Towers, reference V).

Paragraph 35 of the Office Action discusses Claim 38. Claim 38, as one element, includes "wherein ... the finite field is represented as a field tower." Neither Vanstone nor Koyama discusses field towers. The Office Action asserts that Elkies teaches a finite field represented as a field tower on page 1, paragraphs 1&2.

In fact, Elkies does not discuss field towers. Elkies discusses towers of modular curves, which are mathematical

objects different from the field towers of the present patent application. On page 1, line 6 of the Introduction, he explicitly says that X_0(N) are curves. Curves are not finite fields.

To see one example of the different properties of Elkies' modular curve towers from the present patent application's field towers: Field towers have the property that each field within the tower is isomorphically contained in the next larger field, and that the number of elements of the larger field is a power of the number of elements of the smaller field. The fields GF[2^3] and GF[2^6] could be adjacent in a field tower because 64 (= 2^6) is a power of 8 (= 2^3). But GF[2^3] and GF[2^4] could not be in the same field tower because 16 is not a power of 8. Elkies' modular curve towers are illustrated in his equation 2 (page 2), where the number of elements in the tower objects (modular curves X_0(l^n)) are consecutive powers of the prime l (letter el). But l^3 is not a power of l^2, so this modular curve tower cannot possibly be a field tower.

Moreover, since Elkies does not mention any aspect of encryption or concealment of information, and neither Koyama nor Vanstone mentions modular curves in the meaning of Elkies, it makes no sense to combine the references. Also, since none of the three cited references discusses field towers, an essential element is missing from any hypothetical combination.

Applicant submits that Claim 38 is distinguished over the combination of cited arts, and requests withdrawal of this rejection. Claims 39-41 depend on Claim 38. Applicant requests withdrawal of the rejections of dependent Claims 39-41.

Paragraph 38 of the Office Action discusses Claim 41, and asserts that Elkies teaches accelerated arithmetic in an inner field using pre-computed tables. But Elkies does not discuss field arithmetic at all, nor accelerated field arithmetic using precomputed tables.

Applicant submits that Claim 41 is distinguished over the cited arts, and requests withdrawal of the rejection of Claim 41.

CONCLUSION

By this paper, Claims 1, 29, and 59 have been amended to more fully distinguish the invention. Claim 26 is already distinguished over the cited art. Claims 2-28 and 30-58 are dependent upon claims 1, 26, and 29.

Applicant respectfully requests reconsideration of Claims 1-59 as amended. For reasons set forth above, Claims 1-59 are believed to be in condition for immediate allowance, and Applicant so requests.

In the event the Examiner finds any remaining impediment to the prompt allowance of any of these Claims, which could be clarified in a telephone conference, the Examiner is respectfully urged to initiate the same with the undersigned.

DATED this 30th day of November, 2005.

Respectfully submitted,

Richard Schroeppel

Richard Schroeppel, Applicant
500 S. Maple Drive
Woodland Hills, Utah 84653
Telephone: 801-423-7998
Date: November 30, 2005